图书情报工作 ChinaXiv合作期刊
第63卷 第2期 2019年1月

欧盟数据保护官制度研究*

肖冬梅 成思雯
湘潭大学法学院 湘潭 411105

摘要：［**目的/意义**］欧盟数据保护新规(GDPR)中的数据保护官(DPO)制度颇受关注。追溯DPO制度演进路径，剖析DPO的设置与具体职责，考察欧盟DPO制度实施与影响，不止关乎中国企业对欧贸易，更是我国相关规则体系构建的重要参考。［**方法/过程**］通过梳理GDPR中有关DPO的条款及相关过程文本，发现在GDPR规定的3种情形下，数据控制者/处理者应设置数据保护官。DPO的职责包括对数据控制者相关工作人员的告知和建议、监督数据处理的合规性、联络数据主体、同监管机构合作、数据处理活动的记录与归档、培训以及保密等。［**结果/结论**］设置DPO对于确保数据控制者的合规、减轻监管机构负担影响深远。欧盟DPO制度对中国企业/机构的启示在于：应按GDPR的规定设置DPO，并设计完整的数据保护监督流程；对中国数据保护监督及机制建设的启示包括：明确规定数据控制者应设置数据保护专门岗位和专业人员、对不合规的数据控制者给予相应的责任追究和惩罚、加强数据监管机构的建设。

关键词： 数据保护官 个人数据保护 合规性
分类号： G250
DOI:10.13266/j.issn.0252-3116.2019.02.016

1 引言

移动互联网的飞速发展和各种智能终端的广泛普及，使得人类社会快步进入大数据、物联网时代。大数据的收集、处理和利用活动深入渗透到医疗、科技、教育、体育、商业、经济等社会生活的各个领域，全球化的数据洪流正向我们奔涌而来。大数据能让世界更加透明，拥有越多的数据，就意味着能更精准地认识世界、预测未来，许多以往我们难解的社会问题也能迎刃而解，但大数据给我们带来数据红利的同时，也给传统国家封闭的疆界和国家安全带来严重挑战[1]。2016年欧盟《统一数据保护条例》(*General data protection regulation*, GDPR)的出台表明了大数据时代欧盟对于个人数据保护的立场。GDPR改变了之前计算机自动处理数据背景下的数据保护规则，建立起回应大数据时代亟需的更为严格的数据保护框架[2]。

数据保护官(data protection officer，下文简称DPO)的设置是GDPR中的重要条款之一，通过DPO对数据控制者(单独或两个以上共同确定个人数据处理目的和方式的自然人、法人、公共权力机关、代理机构或其他机构)或数据处理者(代表数据控制者处理个人数据的自然人、法人、公共权力机关、代理机构或其他机构)内部的数据处理活动进行合规性监督，加强数据收集处理环节中的保护力度。该条款在整个欧盟数据保护框架中占据重要地位，颇受相关企业和实务部门的关注，不少新闻媒体的报道和社交网络的帖子都在热议DPO。但文献检索结果表明，与此相关的学术成果至今却还寥寥无几，国外学术界除E. Lachaud[3]、R. Miguel[4]少数几位学者对DPO的法律地位、义务以及责任等相关问题进行了初步分析外，与此相关的深度研究成果尚未发现。迄今为止，国内除了在相关文章中提到过DPO制度[5-6]，尚未发现专门研究DPO的学术论文。虽然目前学术界对DPO制度关注似乎不够，但随着GDPR自2018年5月25日正式实施，其影响将日益凸显，DPO制度运行及其相关理论问题的解决将愈发重要，这不止关乎中国企业的对欧贸易，更有助于推进能平衡中国数据经济发展与数据保护的规则建构。

* 本文系国家社会科学基金重点项目"云环境下数字学术信息资源安全的法律保障体系研究"(项目编号：14AZD076)研究成果之一。
作者简介：肖冬梅(ORCID:0000-0001-7611-2058)，院长，教授，法治湖南建设与区域社会管理协调创新中心研究员，E-mail:86650210@qq.com；成思雯(ORCID:0000-0002-7589-1763)，硕士研究生。
收稿日期：2018-06-09 修回日期：2018-08-06 本文起止页码：144-152 本文责任编辑：易飞

中国是欧盟的重要贸易伙伴,我国企业拓展欧洲市场时必然涉及对欧盟公民个人数据的收集和处理,各跨国企业应当严格遵守 GDPR 的规定。通过解读 GDPR 中 DPO 的相关规定,分析 DPO 的设置规则及其在确保合规上的基础性作用,有利于我国企业合规处理欧盟公民的个人数据,能有效防控我国企业在中欧贸易中的违规风险。尤为重要的是,随着我国《网络安全法》《民法总则》等相关法律相继回应大数据时代的需求,确立了个人数据保护条款,毋庸置疑,这些偏原则性的立法的真正落地需要与之配套的具体规则体系,因此当前我国构建能平衡数字经济发展与个人数据权利的数据保护法律体系的任务日益紧迫,深入研究数据保护领域的先行者——欧盟创设的 DPO 制度,为我国构建数据保护法律体系提供借鉴和参考,可谓意义深远。

2 欧盟 DPO 制度溯源

2.1 DPO 在欧盟的早期发展

早期的个人数据被划归为隐私权范畴。随着个人数据收集和使用的急剧增加,对传统"私人领域"产生了巨大冲击。"个人数据在隐私权的范畴下,缺乏对抗公、私主体信息滥用行为的有效权能"[7],世界上大部分国家开始关注个人数据保护问题。20 世纪 70 年代,欧洲各国开始进行个人数据保护立法与制度建设,其中以德国最为典型。1977 年德国《联邦数据保护法》首次出现 DPO(在德语中表达为"beauftragter für den datenschutz")一词,规定其作用为确保数据控制者遵守数据保护条款。2001 年德国对《联邦数据保护法》进行修改,明确规定"公共机关和私人机构应当为 DPO 行使职责提供支持"[8],DPO 逐渐受到重视。进入 21 世纪之后,社交网络、云计算逐渐兴起,黑色数据产业链也逐渐形成。德国国内用户数据泄露、数据非法交易等乱象丛生,2009 年德国联邦议会再次对《联邦数据保护法》进行修改。该次修改提高了 DPO 的法律地位,同时赋予了 DPO 更多权力。

除德国之外,欧洲其他国家的数据保护立法也存在 DPO 或类似概念,从设置类型上可划分为强制性 DPO 和非强制性 DPO 两类。强制性 DPO 是指法律明文规定在一定条件下必须设置 DPO 职位,比利时、西班牙和匈牙利等国采用这一模式。比利时《数据保护法案》(Data protection act 1992)及其之后颁布的法令和修正案规定需大规模收集处理公民个人数据的组织和团体应当设置 DPO 以保证合规;西班牙《数据保护法》(*Data protection act 1999*)规定处理某些类别数据(刑事犯罪相关数据、信誉服务相关数据、税务相关数据、金融相关数据、社保相关数据、涉及一系列个人相关数据等 11 项)时,必须设置"安全官"(security officer);匈牙利《个人数据保护和公共数据公示法》(*Act LXIII of 1992 on the protection of personal data and the publicity of public data*)第 28 条和第 31A 条明确规定在 4 种情形(处理国家主管部门、国家劳工或国家犯罪的数据文件时;金融机构;电信服务提供商;公共事业服务提供者)应当设置 DPO。非强制性 DPO 是指数据控制者可以根据自身情况选择是否设置 DPO,英国、法国、瑞典等国采用该模式。

2.2 GDPR 制定过程中有关 DPO 条款的争议

1995 年欧盟《有关个人数据处理中的个人保护和所涉数据自由流通指令》(Directive 95/46/EC)的制定立足于计算机自动处理个人数据,时至今日其已无法应对各种新型数据风险。2010 年起,欧盟开始全面检讨其个人数据保护框架。2012 年 1 月欧盟委员会(The European commission)向欧盟理事会(The European council)提交《欧盟议会和欧盟理事会关于规范个人数据处理中个人保护和所涉数据自由流通的条例建议案》(下文简称 GDPR《草案》)。GDPR《草案》首次将 DPO 写入欧盟统一数据保护立法,在此后 4 年的商议和修改中,DPO 一直是修法争论的焦点。

DPO 设置的争议主要在两个方面:①哪些数据控制者应当设置 DPO;②是否要强制满足条件的数据控制者设置 DPO。GDPR《草案》第 35 条第 1 款明确 3 类数据控制者应当设置 DPO,其(b)项规定,"雇员超过 250 人的企业应当设置 DPO"。英国、法国等国家认为设置 DPO 应持自愿态度,强制无疑会增加数据控制者额外的负担[9]。英国信息专员办公室((information commissioner's office,ICO)认为:企业如果具有确保数据保护合规性的有效流程,则不必设置专门的 DPO,是否设置 DPO 应当取决于是否有必要通过 DPO 来实现合规要求,而不是简单考虑员工人数[10]。德国、匈牙利等国家则倾向于采取强制性规定,强制性规定对数据控制者的规制更加严格,更符合 GDPR 的立法目的。因为这些争议,欧洲议会在法案审议中进一步提升了设置 DPO 的门槛:若数据控制者连续 12 个月内涉及处理超过 5 000 名数据主体的个人数据时应当设置 DPO[11]。

3 DPO 的设置与职责

3.1 DPO 的设置

3.1.1 设置 DPO 的主体 GDPR 第 37 条第 1 款规定在以下 3 种情形时，数据控制者/处理者应当设置 DPO：①需要进行数据处理的主体是行政机关或公共团体(法院除外)；②数据控制者或数据处理者的核心业务由数据处理组成，且因其性质、经营范围或设立目的等需要对数据主体进行定期、系统大规模监测时；③数据控制者或数据处理者的核心业务为处理大规模特殊类型数据、或处理与违法犯罪定罪量刑有关数据时。

(1)行政机关或公共团体。GDPR 第 37 条第 3 款规定，数据控制者/处理者为行政机关或公共团体时应当设置 DPO，但考虑其组织形式和政府行政成本，通常多个机关或团体共同设置一名 DPO，但法院在行使其司法职能中所涉及的数据处理活动不在此范围。

(2)私有企业或团体。针对私有企业或团体，不同数据控制者的经营范围/设立目的不同，对于数据处理的要求也不同。GDPR 规定：若企业核心业务为数据处理，且需要对数据主体进行定期、系统大规模监测时应当设置 DPO，在实践中应当综合企业数据处理活动的规模、监测数据主体的时间、涉及数据主体的数量等多项因素综合考虑。

由于各成员国之间存在国情和数据保护政策的差异，“DPO 作为企业的门面，在不同国家要求通晓当地的语言且了解当地实情”[12]。针对跨国或者跨区域企业集团，通常认为该企业集团在同一国家内的多个实体仅设置一名 DPO，且应当确保 DPO 克服地方差异，与不同成员国内的实体保持紧密联系。针对非欧盟数据控制者，在数据主体所在成员国内应当设置一名 DPO。

针对大规模处理特殊类别数据及与刑事定罪和犯罪有关数据的数据控制者或处理者，由于数据类型的特殊性，其数据处理活动的合规性愈加重要，应当设置 DPO 来进行严格监督和管理。其他各类数据控制者或数据处理者可以按照欧盟或成员国法律的要求设置 DPO 履行相应的职责。

3.1.2 DPO 的类型

(1)内部 DPO 与外部 DPO。根据 DPO 是否是数据控制者的员工可将 DPO 分为内部 DPO(internal DPO)和外部 DPO(external DPO)。DPO 不仅需要熟悉数据控制者内部的数据处理活动，还需要熟悉数据控制者的基本运作，并有效地将二者结合。内部 DPO 是数据控制者的员工，熟悉其内部基本运作。但由于之前不同的工作背景，内部 DPO 的数据保护知识和实务经验相对缺乏，数据控制者需要通过培训等措施来提高其专业素养，合规成本相对提高。外部 DPO 通常为专业的服务机构或律师事务所，专业知识和实务经验丰富。GDPR 规定 DPO 不得因履行职责而被处罚或被解雇。但内部 DPO 与数据控制者之间是雇佣关系，同样适用成员国劳动法和企业章程，DPO 若因履行数据保护职责之外的其他原因违反劳动法或公司章程，数据控制者仍可单方面解除劳动合同(劳动合同的单方面终止仅适用于例如严重违反非披露义务或偷窃、歧视其他员工或存在其他重大过失的情形。一般情况下适用 GDPR 的规定，不可因履行职务而受处罚或被解雇)。外部 DPO 与数据控制者之间基于服务合同来履行职责，双方可以针对限制性条款自行约定并达成合意，相对于内部 DPO 来说会更加自由。通常大型企业选择设置内部 DPO，而中小型企业为了减少合规成本大多外聘 DPO 来对特定数据处理活动进行监督管理。

(2)兼职 DPO 与全职 DPO。根据是否专门从事 DPO 的工作可将 DPO 分为兼职(part-time DPO)和全职 DPO(full-time DPO)。兼职 DPO 的设置相对灵活，在一定程度上可以降低数据控制者的合规成本，但在其 DPO 职责与非 DPO 职责之间会产生包括时间分配、精力分配和利益冲突等矛盾。全职 DPO 更为专一尽职，更有利于个人数据的保护，但企业投入成本相应增加，对于小型企业而言负担过重。在实践中，数据控制者应当具体情况具体分析，选择合适的 DPO 类型，一要保证达到合规要求，二要确保数据控制者能够承担得起。

3.1.3 DPO 的专业资质 GDPR 第 37 条第 5 款规定，DPO 应当具备一定专业素养，包括数据保护法的专业知识以及实务操作能力，同时能够胜任所有 DPO 的职责和义务。DPO 需掌握的数据保护法不仅仅局限于 GDPR，还包括其他与数据保护相关的欧盟法规和成员国法律，这些法律法规与 GDPR 相互影响。DPO 应当熟悉数据控制者的所有数据处理活动，了解其运作，并将二者有效地结合。除此之外，DPO 是数据控制者与数据主体、数据保护监管机构之间联系沟通的媒介，精湛的人际交往能力、富有逻辑的语言表达能力、强大的公关能力等都能为 DPO 履行其职责提供有效帮助。

3.2 DPO 的职责及其履行

在令相关主体遵守数据保护要求方面，DPO 起着不可或缺的作用。一方面 DPO 要确认数据控制者的

义务,提供合规性建议,独立监督数据控制者内部各项数据处理活动是否按照数据保护规则进行;另一方面,DPO 作为数据主体和监管机构的联络点,是数据主体联系数据控制者的媒介,同时与监管机构保持紧密合作。

3.2.1　DPO 的职责

（1）通知和建议。GDPR 第 39 条第 1 款（a）项规定,为了使数据控制者或其他有义务实施处理行为的工作人员明确其义务和责任,DPO 对其有告知义务,并应提出相关建议。对数据控制者来说,DPO 应当告知有关数据保护的一般性政策及其实时更新情况;就有关数据保护的切实可行的改进措施向数据控制者或处理者提出建议;就数据保护条款的适用提出合规性建议等。对其他有义务实施处理行为的工作人员来说,DPO 应当向所有员工（包括行政工作人员）就一般性义务问题进行告知解释并提出相关建议,包括其自身的个人数据权利（数据保护义务通常指向外部客户、潜在客户等数据主体,但是内部雇员作为数据主体同样享有数据权利）。DPO 接受任何有关条例解释或适用问题的咨询,致力于提升数据控制者及相关人员的数据保护意识,加强数据处理操作过程中的安全性,降低受处罚的风险。

（2）监督数据处理的合规性。GDPR 第 39 条第 1 款（b）项规定,DPO 应当监督数据控制者内部数据处理活动的合规情况。数据控制者内部的数据处理活动不仅要遵守 GDPR 的规定,还要符合其他欧盟数据保护条例、成员国数据保护法以及数据保护政策的要求。DPO 应积极主动监测、评估、审查、修正相关数据保护措施[13]。DPO 可以主动或依请求直接在数据控制者内部调查与数据保护相关的活动,解决相关问题,并将情况汇报给数据控制者的最高管理层。DPO 可以对数据处理活动进行事先检查,监督数据保护影响评估工作的进行并提出建议（GDPR 第 39 条第 1 款（c）项）。DPO 应当监督员工的有关活动,包括:员工在数据处理工作上的职责分配、合规意识的提升以及数据保护知识培训等事务。内部审计（有助于 DPO 了解企业或机构所控制个人数据的类型、位置、访问权限和投诉请求）或者外部审计（通常交第三方组织进行,就法律、IT 等特定问题进行）涉及个人数据的潜在问题和活动也在 DPO 的监督之列。除此之外,DPO 应当适当考虑各项数据处理操作可能存在的风险（GDPR 第 39 条第 2 款）,包括风险的性质、范围、内容。对数据控制者进行合规性监督可以说是 DPO 确保个人数据受到保护的最基础的职责。

（3）联络数据主体。GDPR 第 38 条第 4 款规定,DPO 的一个重要职责是充当数据主体同数据控制者之间的联络点。DPO 不仅要掌握数据保护相关的专业知识,同时也要足够了解数据控制者的内情,了解其内部所有关于数据保护的事项与活动。数据控制者应当将 DPO 的联系方式提供给数据主体,方便数据主体与 DPO 保持密切联系。数据主体可以就其个人数据的处理和本条例规定的有关权利行使的一切问题联络、咨询 DPO。

（4）与监管机构合作。DPO 还应当同监管机构合作（GDPR 第 39 条第 1 款（d）项）,数据控制者应当将 DPO 的联络方式提供给监管机构（GDPR 第 37 条第 7 款）。合作通常包括 3 个方面:①DPO 可以充当监管机构的联络点,处理来自监管机构的问询或投诉,使监管机构可以将相关风险或其他紧急事项及时有效地通知到数据控制者。②DPO 可以就个人数据安全相关的事项向监管机构事先征询,包括审计问题、法律实施问题、一般合规性文件审查问题等。③DPO 应当监督监管机构向数据控制者提出的建议的实施情况、投诉的处理情况,并及时反馈回监管机构。在其权限范围内,DPO 可以就监管机构正在审查的问题调查收集信息。DPO 与监管机构之间是双向促进的工作关系,二者之间联系越强大,可以解决的个人数据安全问题便越多,权利被侵害的风险便越小。

（5）数据处理活动的记录与归档。数据处理活动的记录与归档在 GDPR 第 37 条第 1 款（d）项有明确规定。数据控制者或处理者需要保存所有的数据处理活动（GDPR 第 30 条第 1 款）。DPO 承担对所有数据处理操作的记录归档工作。记录涉及:数据处理的初始信息、数据处理者和第三方、数据处理的原则宗旨及限制、合法的处理条件、个人数据的集合、一般及特殊个人数据类型、个人数据的定位、相关安全措施、数据的收集和传输、数据的删除和数据的生命周期、数据处理的维护和更新记录、数据处理的作用、培训、记录的保留期限以及相关义务、政策、程序、协议和合同等相关信息。

（6）培训。关于 DPO 的培训在 GDPR 第 39 条第 1 款（b）项有明确规定。DPO 在数据控制者内部需定期开展员工培训。培训的最低标准是使数据控制者内部所有员工了解数据保护的基础知识,具有数据保护的一般水平。根据不同部门对数据保护程度的不同需求,分别进行更为深入的部门培训和意识提升。DPO

需要不断发现各部门日常工作中可能出现的数据问题,并就不同问题结合各部门的工作范围进行数据保护教育。培训方式可以包括:电子邮件、纸质文件、政策宣传、资料更新、数据保护课程、研讨会、具体问题指导和网络课程等[12]。

(7)保密。GDPR 第 38 条第 5 款规定,DPO 应当就其任务的履行承担保密义务,不得泄露其履行职责时获悉的信息和文件,保护个人数据,保护数据主体的隐私。

3.2.2 DPO 的履职保障 为了 DPO 能更好地履行其职责,GDPR 第 38 条第 1 款规定,数据控制者或数据处理者应当确保 DPO 能恰当、及时地参与所有个人数据保护的事务,为其履职提供基本支持和保障。

(1)DPO 的独立地位。数据控制者设置 DPO 的目的在于对其内部的数据处理活动进行合规性监督,这要求 DPO 对数据控制者的数据保护政策、数据处理活动有一个整体且全面的认识。基于此,DPO 在数据控制者内部应当处于相对独立的地位,体现在:①"DPO 需要一条超越涉案上级的汇报线来对相关数据处理活动提出异议"[7],也就是说,DPO 的汇报线(指在企业内部层级结构中,DPO 应当向谁汇报工作、反映情况、提出意见或建议以及回答谁的问询的一种层级关系)直接指向数据控制者或处理者的最高管理层(见 GDPR 第 38 条第 3 款),其不存在直接的上下级,最大限度减少汇报过程中不必要的干扰和指示,这是确保 DPO 独立性的关键。②DPO 不属于数据控制者的任何一个部门,不专门为某一部门服务。DPO 需要对所有部门的数据处理活动进行监督,若 DPO 从属于某一部门,在监督和调查过程中,DPO 作为该部门的一员,其自然也是受调查主体之一,个人利益与企业利益发生冲突则无法保证 DPO 履职的客观性。但并不是说 DPO 应与所有部门完全隔绝,DPO 的工作与其他部门工作之间存在交叉,其与各部门之间的融洽关系也很重要。③DPO 不得因履行数据保护职责而被解雇或受处罚,这是对 DPO 的履职保护。需要注意的是,DPO 所拥有的独立地位是相对的。GDPR 规定 DPO"不接受任何指示"是指其在履行关键任务时的业务独立性。数据控制者根据不同数据处理活动的性质确定不同的数据保护政策和执行程序,DPO 在此范围内帮助数据控制者以合规的方式实现业务目标,自由地提供有关合规的建议,数据控制者是否遵循其建议最终取决于具体的业务标准。

(2)DPO 的资源保障。GDPR 第 38 条第 2 款规定,数据控制者应当为 DPO 提供其所需的独立预算和硬件资源。独立的财政预算用以确保 DPO 职责的顺利履行,必要时,DPO 还可以请求数据控制者批准额外的经费。DPO 应当在各部门拥有对个人数据和处理操作的访问权限,有权对数据控制者内部个人数据进行采集,有权对数据处理操作进行事前检查,数据控制者应予以支持,不得加以限制。为了更好地履行职责,DPO 应当拥有必要的资源支持,例如人力资源、IT 资源、办公设备等。为了加强自身的工作能力和业务水平,DPO 可以要求数据控制者采取一定措施来维持或加强其专业知识,例如组织培训、提供学习机会等。

4 欧盟 DPO 制度的实施将带来的影响

4.1 DPO 需求量激增

GDPR 从 2016 年 4 月 14 日出台到 2018 年 5 月 25 日正式实施的两年多时间内,处于 GDPR 规制下的数据控制者或数据处理者需要完成合规清单,为实施 GDPR 做准备。合规清单中最重要的一项事务便是 DPO 的设置。GDPR 加大对违规行为的处罚力度无疑给所有数据控制者或处理者敲响警钟,从而迫使数据控制者和处理者不得不按 GDPR 的要求来设置 DPO。

2016 年底国际隐私专家协会(International Association of Privacy Professionals, IAPP)的一项研究对即将产生的 DPO 数量进行了估算:首先计算出 13 个非金融行业中大型欧盟企业的大致数量,根据 GDPR 规定的标准假设:①员工不少于 5 000 名的企业将"大规模"处理和监测人力资源数据;②交通运输和仓储行业、住宿和餐饮服务行业、专业科学和技术行业,由于其数据处理活动属于密集型,过半的企业均需要设置一名 DPO;③所有通讯行业的大型企业均需设置一名 DPO,同时假设所有的金融机构和保险企业由于其业务性质均需设置一名 DPO,行政机关或公共团体则按照欧盟"大型"企业的标准计算总量,并假设每 5 个需要一名 DPO。由此保守得出结论:一旦 GDPR 生效,在欧盟内部将至少产生 28 000 名 DPO[14]。

对于非欧盟国家,根据 GDPR 对数据控制者的定义推断:只要非欧盟成员国的数据控制者是为了向欧盟境内可识别的自然人提供商品和服务而收集、处理了其个人数据,或是为了监测欧盟境内可识别的自然人的活动而收集、处理了其个人数据,无论其是否位于欧盟内部都应当受到 GDPR 的规制。根据 IAPP 年度隐私治理报告表明,有 50% 的美国企业需要遵守 GDPR 的规定。使用贸易额概测法,美国占欧洲全球贸易

的17.7%，可以计算其他欧洲主要贸易伙伴可能需要的DPO数量。经估算可知：一旦GDPR生效，将会在全球范围内创造多达75 000个DPO职位[14]。

DPO的需求量激增，但能够胜任DPO职位的人才仍然稀缺。随着GDPR的生效，一场DPO的“人才大战”正在打响。一方面，供不应求的就业市场将会导致DPO的薪水升高，为了保证DPO的专业素养，企业设置DPO的投入成本将会增大，合规成本升高。另一方面，为了增加DPO专业人才的数量，与DPO相关的培训机构、认证机构随之出现，由此将产生一个新行业。

4.2 DPO的设置对数据控制者和监管机构的影响

设置DPO对于确保数据控制者的合规、减轻监管机构负担，意义重大，影响深远。其主要体现在：

4.2.1 事先审查，降低侵权风险 GDPR赋予DPO事先审查的权利，DPO监督数据处理项目的设计，对其进行先期审查、风险评估，在源头减少可能存在的风险，以防止事后受到法律制裁，为数据控制者节约合规成本，减少赔偿支出。当然监管机构仍有权调查DPO的审查和评估，并通过调查验证风险防范的情况。

4.2.2 优化争端解决机制，减轻监管机构负担 GDPR赋予DPO首先处理数据主体申诉的权利，因为DPO更为熟悉数据控制者内部的数据保护要求和情况，数据主体与数据控制者之间的一些微小争端、低额标的诉求可以通过DPO直接进行解决。在一定程度上可以减轻监管机构的工作量，使监管机构集中指导和调查严重违规活动，节约监管资源和成本。数据控制者或处理者也将避免漫长的争端处理程序，提高了审查效率。同时，DPO作为数据主体、监管机构与数据控制者之间的唯一联络点，整个沟通联络过程合理化程度较高，减少了不必要的干扰和冲突。

4.2.3 加强组织内部数据监管系统，提高数据控制者的竞争力 在数据处理过程中，可能存在风险的环节多，但DPO的审查清单详细全面，使数据控制者的数据处理活动有序，确保组织内的合规性，清楚有效地判断其作为数据控制者是否存在过错。数据保护能力逐渐成为衡量市场主体实力的标准之一，DPO的存在既体现企业数据处理规模和数据保护程度，一定程度上也能提高市场主体的竞争力。

GDPR强制在一定条件下设置DPO对于整体数据保护框架是有益的，但其实施可能还存在一些问题。数据控制者数量庞大，其类型、经营范围、资金承受能力、数据保护程度各有不同，“一刀切”的方式对于已经存在有序数据保护流程的数据控制者施加了限制。数据保护规则应当注重调整的是调控结果，而不是过程，DPO的设置是过程调控方式中的优选而不是唯一。对于满足GDPR规定条件的数据控制者，其可能已经有实践效果较好的数据保护流程，或者，虽然没有数据保护相关措施但其运营模式能够将风险限制在可控范围内，此时仍然强制设置DPO无疑是会加大企业运营成本，浪费资源。此外，欧盟各国各地区数据保护程度、发展、政策存在差异，在GDPR出台之前，各国的数据保护立法均经过不断修改已达到适应本国国情的程度。GDPR统一实施之后，可以预见DPO可能出现“水土不服”的现象，若不能正确消解其带来的消极影响，不但会加重企业的合规成本，甚至可能带来违规风险。因此，在GDPR正式实施之际，还有不少问题有待解决。

5 欧盟DPO制度对我国的启示

5.1 欧盟DPO制度对我国企业的启示

中国是欧盟的重要贸易伙伴，中欧贸易占欧盟全球贸易的15%左右。GDPR的实施使得中国企业同样需要做好数据保护专业人才储备和合规准备。中国近年来数据保护研究和数据产业方面有了很大长进和发展，但企业数据保护意识仍然偏弱，这将直接影响中国企业的数据保护水平和合规能力。为了开拓欧洲市场，合法合规地开展中欧贸易，中国相关企业应尽快进行GDPR的合规性评估，制定相应的应对方案来主动适应GDPR的合规性要求。中国相关企业应该按照GDPR的规定，设置类似于DPO的数据保护专岗（员），并设计一套较为完整的数据保护监督流程，制定相应的数据保护与管理制度。

5.1.1 设立数据保护专岗（员） 中国企业可以设立数据保护专岗（员），履行类似于DPO的职责。该岗位人员可以就企业内部个人数据采集、访问、处理、传输等涉及数据安全的问题或事项向管理层提供建议，并负责监督相关事项的实施。对外可以接洽来访者，处理用户（数据主体）或第三方的问询，为其提供可用信息。

5.1.2 记录个人数据处理和流转情况 从个人数据收集起，记录有关该个人数据的所有使用和流转情况。这样做的意义在于：一方面，在记录过程中关注可能存在的风险，方便及时汇报并作好预防；另一方面，便于事后归责。个人数据被侵害后，根据记录可以确定违规操作从而定位责任主体。

5.1.3 建立数据风险预警机制 数据风险预警机制

具体包括事前的风险评估、事中的安全保障措施和事后的补救方案 3 方面。企业采集个人数据之后，作为保障数据安全的义务主体，应当采取一定的措施以履行安全保障义务。不得随意泄露、篡改、毁损其收集的个人数据。应当适当采取技术措施和其他必要措施，防止个人数据的泄露、毁损、丢失。在可能侵害个人数据或已经侵害个人数据的情况下，立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

5.1.4 加强员工培训，提升企业数据保护意识 DPO 的一项重要职责是培训员工，而这在我国有更迫切的需求。我国数据保护近年来虽然有了很大发展，但普及程度低，国民保护意识不强，专业人士较为稀缺。企业通过设置数据保护专岗（员），制定员工培训计划并予以实施，在企业内部普及数据安全知识，提升企业整体数据保护意识。

5.2 欧盟 DPO 制度对我国数据保护制度建设的启示

欧盟是全球通过专门立法进行数据保护的先行者，受其数据保护新规 GDPR 深刻影响和启发的国家包括但不限于中国。“徒法不足以自行”，GDPR 关于数据保护官和数据监管机构的设置和职责设定，旨在为数据主体权利的行使、数据控制者和处理者责任的履行提供专业人才队伍和监管机制的保障。GDPR 颁布两年多之后才正式实施，这是为相关主体依法配备有资质的 DPO 提供必要的过渡期，因为专业人员和专门机构的建设不是一蹴而就的。欧盟创设的 DPO 制度，对我国数据保护制度建设至少有两个方面的启示：①通过立法明确数据控制者/处理者设置类似于 DPO 的数据保护专岗（员）的义务，并规定数据保护专门岗位和专业人员的职责与履职，对数据保护专岗（员）设置不合规的数据控制者和处理者给予相应的责任追究和惩罚；②加强数据监管体系建设，发挥数据控制者/处理者的数据保护专岗（员）的作用。

5.2.1 明确数据控制者设置数据保护岗（员）的义务与责任

（1）把数据保护专门岗位的设置以及专业人员的配备设定为具有一定规模和特殊类型的数据控制者和处理者的一项义务。目前我国虽然在《网络安全法》及其他相关法中赋予了网络运营商等数据控制者和处理者数据保护的责任和义务，但迄今未明确数据保护的义务主体设置数据保护专门岗位和专业人员的相关规定，缺乏专门岗位和专业人员，很容易导致法律法规的执行打折扣，甚至得不到有效执行，这样有法不行、执法不力会严重损害法律的权威。

（2）明确规定数据保护专门岗位和专业人员的职责与履职要求。欧盟 DPO 制度对数据保护官的职责和履行都有明确规定：“公共组织（法院除外）、核心业务涉及对用户进行经常性的大规模的系统性监控的企业、核心业务涉及处理个人敏感数据或者与刑事犯罪有关的个人数据的企业，应当任命一个数据保护官。多个相关企业可以委任一个数据保护官。数据保护官的职责包括通知和建议企业履行其在 GDPR 之下的义务、监测企业履行其义务以及与监管部门合作。”这在很大程度上确保了 GDPR 这个数据保护新规具有很强的操作性，对于数据保护这样的新领域，DPO 事实上已经细化到“要配备什么人（岗位）、有什么职责，应该做什么事、怎么做这些事”，这样周密的制度安排才能确保 GDPR 的有效实施。我国在数据保护制度建设过程中若能明确数据保护专门岗位和专业人员的职责与履职要求，将使得义务主体职责明晰，有助于其明明白白履行义务。

（3）明确对数据保护专岗（员）设置不合规的数据控制者和处理者给予相应的责任追究和惩罚。GDPR 的惩罚措施——违反 GDPR 的企业最高将面临其全球年收入 4% 或 2 000 万欧元的巨额罚款。无强制则无保障，无惩罚则无威慑。GDPR 已经为数据控制者与处理者画出一张数据保护的操作红图，明确的责任追究和高额罚单无疑直指“执法不严、违法不究”的侥幸心理，对滥用数据的行为进行严厉规制，对个人数据的保护提供强有力的保障。而我国《网络安全法》设立的事后处罚标准过低，很难起到应有的威慑作用。我国在后续的相关立法中，可借鉴 GDPR 的责任追究和惩罚措施，以加强对数据滥用行为的规制。

5.2.2 加强数据监管体系建设，发挥数据控制者/处理者的数据保护专岗（员）的作用 从上文有关欧盟 DPO 制度的剖析可知，加强数据监管体系建设，明确数据监管机构的权力与边界，重视 DPO 与数据监管机构的合作，是欧盟数据保护新规的有力举措。从欧盟 DPO 制度设计来看，DPO 与数据监管机构的合作十分重要。即便有周密的 DPO 制度，但若缺少必要的监管机构及相应的制度安排，DPO 的功能也难以得到有效发挥。DPO 是数据主体、监管机构与数据控制者/处理者之间的联络者，也是监管机构任务的分担者（微小争端、低额标的诉求的解决），监管机构也对 DPO 负有指导和咨询之责。GDPR 赋予了数据监管机关以调查、矫正、处罚等权力，也明确了监管机构与 DPO 的分工与合作，其旨在更好地保护数据主体的权利，这对我国

正在探索中的数据监管体系的建设,尤其是数据监管机构的权力和边界的划定,该体系中不同主体之间的分工与合作的规定,有重要的借鉴意义。

6 结语

DPO 制度对确保企业内部的个人数据安全起着基础且关键性的作用。由于 GDPR 明确采用"属人管辖"而非"属地管辖",因此其主张的效力范围不止欧盟及其成员国,欧盟乃至全球相关数据控制者/处理者均有必要设置 DPO,这不仅是对数据主体的数据安全负责,也是企业对数据风险进行防控,并赢得用户信任、确保自身在市场上的竞争力的必由之路。欧盟一直走在数据保护立法的前沿,GDPR 堪称全球数据保护立法的样本,对各个主要国家的立法影响可谓深远。可结合我国国情进行法律移植与创新,探索欧盟 DPO 制度的本土化路径,将其转化为适合我国数据保护需求的制度,推进我国数据安全的保障体系的建设与完善。

参考文献:

[1] 肖冬梅. 在全球数据洪流中筑牢数据边疆[N]. 中国社会科学报,2016-11-10(1).
[2] 高富平. 个人数据保护和利用国际规则:源流和趋势[M]. 北京:法律出版社,2016.
[3] LACHAUD E. Certification of data protection officers should be regulated[EB/OL]. [2018-05-10]. https://ssrn.com/abstract=3176471 or http://dx.doi.org/10.2139/ssrn.3176471.
[4] MIGUEL R. Data protection officer: the key figure to ensure data protection and accountability[J]. European data protection law review,2017,3(1):114-118.
[5] 王融. 大数据时代:欧盟能否重建数据保护新秩序[J]. 中国信息安全, 2016(1):125-127.
[6] 张敏, 马民虎. 欧盟数据保护立法改革之发展趋势分析[J]. 网络与信息安全学报, 2016, 2(2):8-15.
[7] 李欣倩. 德国个人信息立法的历史分析及最新发展[J]. 东方法学, 2016(6):116-123.
[8] CEDPO. Comparative analysis of data protection officials role and status in the EU and More-I[EB/OL]. [2017-05-19]. http://www.cedpo.eu/wp-content/uploads/2015/01/CEDPO_Studies_Comparative-Analysis_DPO_20120206.pdf.
[9] MoJ wants obligation to appoint data protection officers scrapped from EU reform proposals.[EB/OL]. [2017-04-11]. https://www.out-law.com/en/articles/2013/january/moj-wants-obligation-to-appoint-data-protection-officers-scrapped-from-eu-reform-proposals/.
[10] ANGELIQUE C. Where should the new mandatory DPO sit? [EB/OL]. [2017-01-21]. https://iapp.org/news/a/where-should-the-new-mandatory-dpo-sit/.
[11] European Parliament and of the Council. European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [EB/OL]. [2017-07-20]. http://www.europarl.europa.eu/sides/getDoc.do? type=TA&language=EN&reference=P7-TA-2014-0212.
[12] 中国商业电讯. 欧盟 GDPR 留给中国企业的时间不多了[EB/OL].[2017-03-15]. http://www.sohu.com/a/124637983_115007.
[13] PAUL L. The data protection officer: profession, rules, and role [M]. New York:Auerbach Publication,2016.
[14] HEIMES R,PFEIFLE S. Study: GDPR's global reach to require at least 75,000 DPOs worldwide[EB/OL]. [2017-03-20]. https://iapp.org/news/a/study-gdprs-global-reach-to-require-at-least-75000-dpos-worldwide/.

作者贡献说明:
肖冬梅:负责全文构思、部分章节的起草和全文的修改;
成思雯:参与全文谋篇布局、法条梳理以及部分章节的起草。

EU Data Protection Officer: Responsibility, Impact and Enlightenment

Xiao Dongmei　Cheng Siwen
Law School of Xiangtan University, Xiangtan 411105

Abstract: [**Purpose/significance**] The data protection officer (DPO) in the new regulation of EU data protection (GDPR) has attracted considerable attention. Tracing the evolution path of DPO, analyzing the settings and specific responsibilities of it. Studying on DPO system is not only related to trade between China and Europe, but also an important reference for the construction of relevant rules system in China. [**Method/process**] By teasing out the terms of DPO in the GDPR and related texts, in the three cases specified by GDPR, the data controllers or processors should set up DPO. The responsibilities of the DPO include that informing and advising to the data controller's relevant staff, monitoring the compliance of data processing, contacting with data subject, cooperating with the supervisory authority, maintaining re-

cords and documentation of data processing, training, and confidentiality obligation. [**Result/conclusion**] Setting up DPO has far-reaching influence on ensuring the compliance of data controllers and reducing the burden of the supervisory authority. The enlightenment of DPO for Chinese enterprises or institutions is that DPO should be set up according to the provisions of GDPR, and a complete data protection supervision system should be designed as soon as possible. As for the data protection supervision system and mechanism construction in China, it should be clearly stipulated that the data controllers have to set up special posts and professionals for data protection, and investigate and punish non-compliant data controllers with corresponding responsibilities. Meanwhile the construction of data supervisory authority should be strengthened.

Keywords: data protection officer personal data protection compliance

《图书情报工作》2018 年优秀审稿专家

2018 年,有近 300 位审稿专家参加了《图书情报工作》稿件的同行评议工作,共评审稿件 1 400 余篇次,审阅 6 篇及以上的专家有 100 余位。高效、高质量的评审为《图书情报工作》遴选高质量稿件提供了保障。综合考虑今年以来的审稿数量、质量和时效,评选出 50 位 2018 年优秀审稿专家(名单如下)。《图书情报工作》为优秀审稿专家颁发证书并免费赠送一年期刊的电子版。感谢所有审稿专家对《图书情报工作》的大力支持!

(以下优秀审稿专家按姓名拼音排序):

姓名	工作单位
白如江	山东理工大学科技信息研究所
曹锦丹	吉林大学公共卫生学院
崔宇红	北京理工大学图书馆
邓胜利	武汉大学信息管理学院
邓小昭	西南大学计算机与信息科学学院
范爱红	清华大学图书馆
方向明	上海大学图书馆
冯　佳	上海社会科学院文学研究所
甘春梅	中山大学
高　凡	西南交通大学图书馆
韩　毅	西南大学计算机与信息科学学院
胡昌平	武汉大学信息资源研究中心
黄　崑	北京师范大学政府管理学院
黄国彬	北京师范大学政府管理学院
黄令贺	河北大学管理学院
姜春林	大连理工大学人文与社会科学学部科学学与科技管理研究所
李　刚	南京大学信息管理学院
李　明	南京大学信息管理学院
李　武	上海交通大学媒体与设计学院
李书宁	北京师范大学图书馆
李卓卓	苏州大学
刘　冰	天津师范大学管理学院
刘　勘	中南财经政法大学信息与安全工程学院
刘春丽	中国医科大学图书馆
刘晓娟	北京师范大学政府管理学院
刘雪立	新乡医学院期刊社/河南省科技期刊研究中心
刘兹恒	北京大学信息管理系
马　捷	吉林大学管理学院
马学良	国家图书馆
茆意宏	南京农业大学信息科学技术学院
牟冬梅	吉林大学公共卫生学院
裴　雷	南京大学信息管理学院
秦　鸿	电子科技大学图书馆
任树怀	上海外国语大学图书馆
邵　波	南京大学图书馆
滕广青	东北师范大学信息科学与技术学院
王立学	中国科学技术信息研究所
王晰巍	吉林大学管理学院
王延飞	北京大学信息管理系
吴　红	山东理工大学科技信息研究所
吴振新	中国科学院文献情报中心
向桂林	中国科学院生物物理研究所
闫　慧	中国人民大学信息资源管理学院
杨新涯	重庆大学图书馆
张广钦	北京大学信息管理系
张鹏翼	北京大学信息管理系
张卫东	吉林大学管理学院
赵　飞	北京大学图书馆
赵宇翔	南京理工大学
祝忠明	中国科学院兰州文献情报中心/中国科学院资源环境科学信息中心